

10/067, 740
2/8/02
Junichi HMYASHI

(translation of the front page of the priority document of
Japanese Patent Application No. 2001-034057)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: February 9, 2001

Application Number : Patent Application 2001-034057

[ST.10/C] : [JP 2001-034057]

Applicant(s) : Canon Kabushiki Kaisha

March 1, 2002

Commissioner,

Japan Patent Office

Kouzo OIKAWA

Certification Number 2002-3012178

CFM 2513 US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日 MAY 08 2002
Date of Application 2001年 2月 9日

出願番号
Application Number: 特願2001-034057
[ST.10/C]: [JP2001-034057]

出願人
Applicant(s): キヤノン株式会社

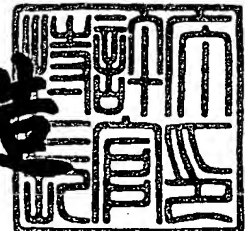
CERTIFIED COPY OF
PRIORITY DOCUMENT

RECEIVED
MAY 10 2002
Technology Center 2100

2002年 3月 1日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 4345005

【提出日】 平成13年 2月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 7/00

【発明の名称】 情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体

【請求項の数】 21

【発明者】

 【住所又は居所】 東京都大田区下丸子3丁目30番2号 キヤノン株式会社
社内

 【氏名】 林 淳一

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100076428

 【弁理士】

 【氏名又は名称】 大塚 康德

 【電話番号】 03-5276-3241

【選任した代理人】

 【識別番号】 100115071

 【弁理士】

 【氏名又は名称】 大塚 康弘

 【電話番号】 03-5276-3241

【手数料の表示】

 【予納台帳番号】 003458

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0001010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体

【特許請求の範囲】

【請求項 1】 デジタル情報に認証情報を付加する情報処理装置であって

付加されるデジタル情報に基づいて認証情報を生成する手段と、

生成された認証情報を、前記デジタル情報に対し、当該デジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記認証情報はデジタル署名であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 更に、前記デジタル情報を秘密鍵を用いて暗号化する暗号化手段を有し、前記デジタル署名は前記デジタル情報を前記秘密鍵で暗号化したデータであることを特徴とする請求項 1 又は 2 に記載の情報処理装置。

【請求項 4】 更に、前記デジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ハッシュ値を秘密鍵を用いて暗号化する暗号化手段を有し、前記デジタル署名は前記デジタル情報のハッシュ値を前記秘密鍵で暗号化したデータであることを特徴とする請求項 1 または 2 に記載の情報処理装置。

【請求項 5】 前記認証情報は、MACであることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】 更に、前記デジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記ハッシュ値を秘密鍵を用いて演算する演算手段を有し、前記 MAC は前記デジタル情報のハッシュ値を前記秘密鍵を用いて演算したデータであることを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】 認証情報は、前記デジタル署名に加えて、更に、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つを含むことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 8】 認証情報が電子透かしとして埋め込まれたデジタル情報を

認証する情報処理装置であって、

前記デジタル情報から電子透かしとして埋め込まれている認証情報を第1の認証情報として抽出する手段と、

抽出された認証情報を電子透かしとして前記デジタル情報から除去し、仮オリジナルデジタル情報に復元する電子透かし除去手段と、

該電子透かし除去手段で電子透かしを除去することで復元された仮オリジナルデジタル情報に基づき、第2の認証情報を生成する生成手段と、

前記第1の認証情報と前記第2の認証情報を比較する比較手段と
を備えることを特徴とする情報処理装置。

【請求項9】 前記第1の認証情報と前記第2の認証情報が等しい時には前記入力されたデジタル情報は改ざんされていない、等しくない場合には改ざんされているとして報知する報知手段とを備えることを特徴とする請求項8に記載の情報処理装置。

【請求項10】 前記認証情報はデジタル署名であることを特徴とする請求項8に記載の情報処理装置。

【請求項11】 更に、前記デジタル署名を公開鍵を用いて復号する復号手段を有し、前記比較手段は、前記第2の認証情報を復号した情報と前記第1の認証情報とを比較することを特徴とする請求項8に記載の情報処理装置。

【請求項12】 更に、前記電子透かしが除去されたデジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記デジタル署名を公開鍵を用いて復号する復号手段を有し、前記認証手段は、前記第2の認証情報を前記公開鍵で復号した情報と前記ハッシュ値とを比較することを特徴とする請求項8に記載の情報処理装置。

【請求項13】 前記認証情報はMACであることを特徴とする請求項8に記載の情報処理装置。

【請求項14】 更に、前記電子透かしが除去されたデジタル情報のハッシュ値を算出するハッシュ値計算手段と、前記MACを秘密鍵を用いて演算する演算手段を有し、前記認証手段は、前記MACを前記秘密鍵で復号した情報と前記ハッシュ値を比較することを特徴とする請求項12に記載の情報処理装置。

【請求項 15】 認証情報は、前記デジタル署名、且つ／或いは、MAC に加えて、更に、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つを含むことを特徴とする請求項 8 に記載の情報処理装置。

【請求項 16】 デジタル情報に認証情報を付加する情報処理装置の制御方法であって、

付加されるデジタル情報に基づいて認証情報を生成する工程と、

生成された認証情報を、前記デジタル情報に対し、当該デジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み工程と

を備えることを特徴とする情報処理装置の制御方法。

【請求項 17】 認証情報が電子透かしとして埋め込まれたデジタル情報を認証する情報処理装置の制御方法であって、

前記デジタル情報から電子透かしとして埋め込まれている認証情報を第 1 の認証情報として抽出する工程と、

抽出された認証情報を電子透かしとして前記デジタル情報から除去し、仮オリジナルデジタル情報に復元する電子透かし除去工程と、

該電子透かし除去工程で電子透かしを除去することで復元された仮オリジナルデジタル情報に基づき、第 2 の認証情報を生成する生成工程と、

前記第 1 の認証情報と前記第 2 の認証情報を比較する比較工程と

を備えることを特徴とする情報処理装置の制御方法。

【請求項 18】 コンピュータが読み込み実行することで、デジタル情報に認証情報を付加する情報処理装置として機能するプログラムであって、

付加されるデジタル情報に基づいて認証情報を生成する工程のプログラムコードと、

生成された認証情報を、前記デジタル情報に対し、当該デジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み工程のプログラムコードと

を備えることを特徴とするコンピュータプログラム。

【請求項 19】 請求項 18 に記載のコンピュータプログラムを格納するこ

とを特徴とする記憶媒体。

【請求項 2 0】 コンピュータが読み込み実行することで、認証情報が電子透かしとして埋め込まれたデジタル情報を認証する情報処理装置として機能するプログラムであって、

前記デジタル情報から電子透かしとして埋め込まれている認証情報を第 1 の認証情報として抽出する工程のプログラムコードと、

抽出された認証情報を電子透かしとして前記デジタル情報から除去し、仮オリジナルデジタル情報に復元する電子透かし除去工程のプログラムコードと、

該電子透かし除去工程で電子透かしを除去することで復元された仮オリジナルデジタル情報に基づき、第 2 の認証情報を生成する生成工程のプログラムコードと、

前記第 1 の認証情報と前記第 2 の認証情報を比較する比較工程のプログラムコードと

を備えることを特徴とするコンピュータプログラム。

【請求項 2 1】 請求項 2 0 に記載のコンピュータプログラムを格納することを特徴とする記憶媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、デジタル情報の署名、及び認証をする情報処理方法及び装置と記憶媒体に関するものである。

【0 0 0 2】

【従来の技術】

近年、コンピュータとそのネットワークの急速な発達及び普及により、文字データ、画像データ、音声データなど、多種の情報がデジタル化されている。デジタル情報は、経年変化などによる劣化がなく、いつまでも完全な状態で保存できる一方で、容易に編集・加工を施すことが可能である。こうしたデジタルデータの編集・加工は利用者にとって有益であることが多い。

【0 0 0 3】

しかしその一方で、例えば、事故処理で証拠写真を扱う保険会社や、建築現場の進捗状況の記録を扱う建設会社においてはデジタルデータの信頼性は従来のアナログデータと比較して低く、証拠としての能力に乏しいという問題を抱えている。

【0004】

そこでデジタルデータの改ざん、偽造が行われていた場合にそれを検出するような映像入力装置、システムが提案されてきた。

【0005】

例えばデジタル署名を利用するシステムは、前記改ざん、偽造を検出するシステムとしてよく知られている。ここでデジタル署名について簡単に説明する。

【0006】

デジタル署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することである。デジタル署名データ生成にハッシュ(Hash)関数と公開鍵暗号を用いたデータの正当性の確認は以下のようなになる。

【0007】

秘密鍵を K_s 、公開鍵を K_p とすると、発信者は、平文データ M をハッシュ関数により圧縮して一定長の出力 h （例えば128ビット）を算出する演算を行う。次に秘密鍵 K_s で h を変換してデジタル署名データ s を作成する演算、すなわち $D(K_s, h) = s$ を行う。その後、該デジタル署名データ s と平文データ M とを送信する。

【0008】

一方受信者は受信したデジタル署名データ s を公開鍵 K_p で変換する演算、すなわち $E(K_p, s) = E(K_p, D(K_s, h')) = h'$ と、受信した平文データ M' を発信者と同じハッシュ関数により圧縮して h' を算出する演算を行い、 h' と h が一致した場合、受信したデータ M' が正当であると判断する。

【0009】

平文データ M が送受信間で改ざんされた場合には $E(K_p, s) = E(K_p, D(K$

$s, h')$))= hh' と、受信した平文データ M' を発信者と同じハッシュ関数により圧縮した h' が一致しないので改ざんを検出できるわけである。

【0010】

ここで、平文データ M の改ざんに合わせてデジタル署名データ s の改ざんも行われてしまうと改ざんの検出ができなくなる。しかし、これは h から平文データ M を求める必要があり、このような計算はハッシュ関数の一方向性により不可能である。以上、説明したように、公開鍵暗号方式とハッシュ関数を用いたデジタル署名によって、正しくデータの認証を行うことが可能である。

【0011】

次にハッシュ関数について説明する。ハッシュ関数は上記デジタル署名の生成を高速化するため等に用いられる。ハッシュ関数は任意の長さの平文データ M に処理を行い、一定の長さの出力 h を出す機能を持つ。ここで、出力 h を平文データ M のハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。ハッシュ関数に要求される性質として、一方向性と衝突耐性が要求される。一方向性とは h を与えた時、 $h=H(M)$ となる平文データ M の算出が計算量的に困難であることである。衝突耐性とは平文データ M を与えた時、 $H(M)=H(M')$ となる平文データ M' ($M \neq M'$)の算出が計算量的に困難であること、及び、 $H(M)=H(M')$ かつ $M \neq M'$ となる平文データ M, M' の算出が計算量的に困難であることである。

【0012】

ハッシュ関数としてはMD-2, MD-4, MD-5, SHA-1, RIPEMD-128, RIPEMD-160等が知られており、これらのアルゴリズムは一般に公開されている。

【0013】

続いて公開鍵暗号について説明する。公開鍵暗号は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の特徴としては、

- (a) 暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。
- (b) 各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に

記憶しておけばよい。

(c) 送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。
が挙げられる。

【0014】

例えば、平文データ M に対して、公開の暗号鍵 K_p を用いた暗号化操作を $E(K_p, M)$ とし、秘密の復号鍵 K_s を用いた復号操作を $D(K_s, M)$ とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

- (1) K_p が与えられたとき、 $E(K_p, M)$ の計算は容易である。 K_s が与えられたとき、 $D(K_s, M)$ の計算は容易である。
- (2) もし K_s を知らないなら、 K_p と E の計算手順と、 $C = E(K_p, M)$ を知っていても、 M を決定することは計算量の点で困難である。

【0015】

次に、上記(1)、(2)に加えて、次の(3)の条件が成立することにより秘密通信が実現できる。

- (3) 全ての平文データ M に対し、 $E(K_p, M)$ が定義でき、 $D(K_s, E(K_p, M)) = M$ が成立する。つまり、 K_p は公開されているため誰もが $E(K_p, M)$ を計算することができるが、 $D(K_s, E(K_p, M))$ を計算して M を得ることができるのは秘密鍵 K_s を持っている本人だけである。一方、上記(1)、(2)に加えて、次の(4)の条件が成立することにより認証通信が実現できる。

- (4) すべての平文データ M に対し、 $D(K_s, M)$ が定義でき、 $E(K_p, D(K_s, M)) = M$ が成立する。つまり、 $D(K_s, M)$ を計算できるのは秘密鍵 K_s を持っている本人のみであり、他の人が偽の秘密鍵 K_s' を用いて $D(K_s', M)$ を計算し K_s を持っている本人になりすましたとしても、 $E(K_p, D(K_s', M)) \neq M$ なので受信者は受けとった情報が不正なものであることを確認できる。また、 $D(K_s, M)$ が改ざんされても $E(K_p, D(K_s, M)') \neq M$ となり、受信者は受けとった情報が不正なものであることを確認できる。

【0016】

上記の秘密通信と認証通信とを行うことができる代表例としてRSA暗号やR暗号

やW暗号等が知られている。

【0017】

ここで、現在最も使用されているRSA暗号の暗号化、復号は次式で示される。

暗号化：暗号化鍵 (e, n) 暗号化変換 $C = M^e \pmod{n}$

復号：復号鍵 (d, n) 復号変換 $M = C^d \pmod{n}$

$n = p \cdot q$ ここで p, q は大きな異なる素数である。

【0018】

上記のように、RSA暗号は暗号化にも復号にもべき乗演算と剰余演算が必要であるので、DESをはじめとする共通鍵暗号と比較すると演算量が膨大なものとなり高速な処理は難しい。

【0019】

以上説明したように、従来技術における改ざん、及び偽造の検出は、デジタルデータに加えて、前記デジタル署名を必要とする方式である。通常、デジタル署名は、デジタルデータのヘッダ部分などに添付する方式で送信することが行われる。しかしながら、デジタルデータのフォーマット変換などによって添付されたデジタル署名は容易に除去される可能性がある。デジタル署名が除去された場合、デジタルデータの認証をすることはできない。

【0020】

これを解決した方法が、特開平10-164549号公報に示されている。特開平10-164549号公報においては、デジタル情報をふたつの領域に分割し、分割された第1の領域からデジタル署名を生成し、生成されたデジタル署名を、分割された第2の領域に電子透かしとして埋め込むことにより、署名が施されたデジタル情報を生成する。一方、認証装置においては、署名が施されたデジタル情報を前記第1の領域と第2の領域に分割し、前記第1の領域から第1のデジタル署名を生成し、第2の領域から電子透かしとして埋め込まれている第2のデジタル署名を抽出する。そして第1のデジタル署名と第2のデジタル署名が等しい時に前記デジタル情報が改ざん、及び偽造されていないことを認証する方法である。

【0021】

【発明が解決しようとする課題】

以上説明したように、デジタルデータの認証をするためには、認証情報をデジタル情報と不可分の状態にしておくことが重要である。前記特開平 1 0 - 1 6 4 5 4 9 号公報の方法においては、オリジナルの画像の認証をするために、電子透かしとして署名情報を埋め込んでおり、更にこの電子透かしは除去することが不可能であるため、オリジナルの画像を得ることは出来ない。アプリケーションや利用者によっては、電子透かしの埋め込み自体を「改ざん」とであると判断する可能性もある。

【 0 0 2 2 】

【課題を解決するための手段】

本発明はかかる問題点に鑑みなされたものであり、認証情報をデジタル情報と不可分にししつつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのデジタル情報に復元することを可能ならしめる情報処理装置及びその制御方法及びコンピュータプログラム及び記憶媒体を提供しようとするものである。

【 0 0 2 3 】

かかる本発明の課題を解決するため、例えば本発明における、認証情報を付加する側の情報処理装置は以下の構成を備える。すなわち、

デジタル情報に認証情報を付加する情報処理装置であって、

付加されるデジタル情報に基づいて認証情報を生成する手段と、

生成された認証情報を、前記デジタル情報に対し、当該デジタル情報が復元可能に電子透かし情報として埋め込む電子透かし埋め込み手段とを備える。

また、認証する側の装置である情報処理装置は以下の構成を備える。すなわち

認証情報が電子透かしとして埋め込まれたデジタル情報を認証する情報処理装置であって、

前記デジタル情報から電子透かしとして埋め込まれている認証情報を第 1 の認証情報として抽出する手段と、

抽出された認証情報を電子透かしとして前記デジタル情報から除去し、仮オリジナルデジタル情報に復元する電子透かし除去手段と、

該電子透かし除去手段で電子透かしを除去することで復元された仮オリジナルデジタル情報に基づき、第 2 の認証情報を生成する生成手段と、

前記第 1 の認証情報と前記第 2 の認証情報を比較する比較手段とを備える。

【 0 0 2 4 】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を詳細に説明する。

【 0 0 2 5 】

以下では、情報に認証情報を埋め込む装置として署名装置、その情報を受けて認証する装置を認証装置として説明する。

【 0 0 2 6 】

<署名装置>

本実施形態における署名装置を図 2 を用いて説明する。

【 0 0 2 7 】

図 2 において、2 0 1 は画像入力部、2 0 2 はハッシュ値計算部、2 0 3 は暗号部、2 0 4 は電子透かし埋め込み部、2 0 5 は画像出力部である。

【 0 0 2 8 】

まず、画像入力部 2 0 1 に対して画像信号がラスタースキャン順に入力される。画像入力部 2 0 1 の入力対象としては、イメージスキャナ、画像が記憶された記憶媒体、遠隔から通信によって受信する通信手段等のいずれでも構わない。以降の説明では画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を有する画像であるならば、RGB 各色成分、或いは、輝度、色度成分を上記単色成分として処理すれば良い。

【 0 0 2 9 】

さて、入力された画像信号 I は、ハッシュ値計算部 2 0 2、及び電子透かし埋め込み部 2 0 4 に出力される。

【 0 0 3 0 】

ハッシュ値計算部 2 0 2 は、入力された画像信号 I のハッシュ値 H を計算して

出力するものである。ハッシュ値Hを算出するためにハッシュ関数を用いられるが、本発明においてハッシュ関数は特に限定されることなく、一般に公開されているMD-2、MD-4、MD-5、SHA-1、PIPEMD-128、PIPEMD-160など種々の方式を用いることが可能である。算出されたハッシュ値Hは暗号部203に出力される。

【0031】

暗号部203は、入力されたハッシュ値Hを秘密鍵Sを用いて暗号化して出力するものである。本発明において暗号化をするための暗号アルゴリズムは特に限定されることなく、例えば公開鍵暗号であるRSA暗号などを用いることが可能である。暗号化されたハッシュ値E_s(H)は電子透かし埋め込み部204に出力される。

【0032】

電子透かし埋め込み部204は、入力された画像信号Iに前記暗号化されたハッシュ値E_s(H)を可逆の電子透かしとして埋め込み出力する（可逆の電子透かしの詳細な説明は後述する）。電子透かしが埋め込まれた画像信号wIは、画像出力部205に出力される。出力対象は、記憶媒体、通信回線等で構わないし、その対象は特に限定されない。

【0033】

<認証装置>

次に、本実施形態における認証装置について図3を用いて説明する。

【0034】

図3において、301は画像入力部、302は電子透かし抽出部、303は復号部、304はハッシュ値計算部、305は比較部である。

【0035】

まず、画像入力部201に対して画像信号wI'がラスタースキャン順で入力される。入力された画像wI'は電子透かし抽出部302に出力される。ここでwI'とは、望ましくは図2に示した署名装置の出力wIに等しいものであるが、改ざん、及び偽造されている場合をも想定して、ここではwI'と表現している。

【0036】

電子透かし抽出部 302 は、入力された画像信号 wI' から埋め込まれている電子透かし $E's(H)$ を抽出し、更に可逆の電子透かしを除去するものである。抽出された電子透かし $E's(H)$ 、及び電子透かしが除去された画像データ I' が出力される。

【0037】

ここで、 wI' が wI に等しい場合には、電子透かしとして $E's(H)$ が抽出される（即ち、 $E's(H) = E's(H)$ である）。更に、この場合には可逆の電子透かしは完全に除去され、画像データ I が出力される（即ち、 $I = I'$ である）。一方で、 wI' が wI とは異なる場合には、電子透かしとして $E's(H)$ とは異なるデータが出力される（即ち、 $E's(H) \neq E's(H)$ である）。更に、この場合には可逆の電子透かしは完全に除去されない（即ち、 $I \neq I'$ である）。

【0038】

更に、電子透かし抽出部 302 は、入力された画像データに電子透かしが埋め込まれているか否かを検出する機能を有する。この機能を用いて、 wI' としてデジタル署名が電子透かしとして埋め込まれていない画像データが入力された場合には、電子透かし抽出部は、「情報なし」と出力し、その後の認証処理を実行しない。この場合、モニタなどを用いて、「画像データが認証できない」という表示を出力することも可能である。

【0039】

以上の様に抽出された電子透かし $E's(H)$ は復号部 303 に出力され、電子透かしが除去された画像データ I' はハッシュ値計算部 304 に出力される。

【0040】

復号部 303 は、入力されたデータ $E's(H)$ を復号して出力するものである。復号に際しては、署名装置において用いられた秘密鍵 s に対応する公開鍵 p が用いられる。復号されたデータは比較部 305 に出力される。

【0041】

ハッシュ値計算部 304 は、入力された画像データ I' のハッシュ値 H' を計算して出力するものである。ハッシュ値を算出するためのハッシュ関数としては、

前記署名装置で用いられたものに等しいハッシュ関数が用いられる。算出されたハッシュ値 H' は比較部 3 0 5 に出力される。

【 0 0 4 2 】

比較部 3 0 5 は、入力されたハッシュ値 H と H' を比較することにより、 $w I'$ が改ざん、或いは偽造されたものかどうかを検証するものである。ここで、 H と H' が等しい場合には $w I = w I'$ であり、即ち改ざん、或いは偽造されたものではないと判断する。一方で、 H と H' が異なる場合には $w I \neq w I'$ であり、即ち改ざん、或いは偽造されたものと判断する。この場合、その旨を例えば表示装置に表示する。

【 0 0 4 3 】

<電子透かし埋め込み部>

次に本実施形態における電子透かし埋め込み部 2 0 4 の詳細について説明する。実施形態における、電子透かし埋め込み部で行う処理を簡単に説明すると、電子透かし埋め込み前の画像データにまで完全に復活することができるように、情報を埋め込むものである。

【 0 0 4 4 】

図 4 は電子透かし埋め込み部 2 0 4 の内部構成を示した図である。以下、同図に従って処理の流れを説明する。

【 0 0 4 5 】

画像データ I は電子透かし埋め込み部 2 0 4 に入力され、画像データ I に埋め込む電子透かしの埋め込み位置が、埋め込み位置決定部 4 0 1 で決定される。次に画像データ I は付加情報埋め込み部 4 0 2 に入力され、付加される情報 E_s (H) に従って、前段の埋め込み位置決定部 4 0 1 で決定された位置に電子透かしが埋め込まれる。

【 0 0 4 6 】

そのため、埋め込み位置決定部 4 0 1 は、入力された画像データ I 、画像中に付加情報 E_s (H) を埋め込む位置を表すデータ（各領域を特定する座標と大きさ）を付加情報埋め込み部 4 0 2 に出力する。

【 0 0 4 7 】

付加情報埋め込み部 4 0 2 には、上記画像データ I に加えて、付加情報 E s (H) (複数のビット情報) を入力する。この付加情報 E s (H) は、画像データ I における上記決定された埋め込み位置に、電子透かし技術を用いて埋め込まれる。この電子透かしの技術を用いた付加情報 E s (H) の埋め込みについては後述する。付加情報埋め込み部 4 0 2 からは付加情報 E s (H) が埋め込まれた電子透かし埋め込みデータ w I が出力されることになる。

【 0 0 4 8 】

なお、本実施形態では、電子透かし埋め込み装置に入力するデータは、説明を簡単にするため、1画素が8ビット階調(256階調)を持つグレースケール画像データであるとする。しかし、入力されるデータは、カラー画像データであっても構わない。カラー画像が入力される場合には、カラー画像の1チャンネルの画素値、またはカラー画像の輝度値などを用いることで、同様の埋め込みを行うことが可能である。

【 0 0 4 9 】

また、音声データが入力される場合には、画像の二次元の位置情報を、時間の1次元の情報に置き換えて考えればよく、同様の手法で実現することが可能である。また、動画データが入力される場合には、2次元画像が複数、時間軸に並べられていると解釈することが出来るため、各2次元画像を同様の手法で処理することにより、基本的に、適用可能である。従って、カラー画像、音声、動画に電子透かしの埋め込みを行う場合も、本発明の範疇に含まれる。

【 0 0 5 0 】

次に、本実施形態における、電子透かし埋め込み、電子透かし分離(抽出)の基本原理について説明する。

【 0 0 5 1 】

＜パッチワーク法＞

本実施形態では付加情報 Inf (上記実施形態での E s (H) が対応する) の埋め込みの為にパッチワーク法と呼ばれる原理を用いている。パッチワーク法については、論文「電子透かしを支えるデータ・ハイディング技術(上)」Walter Bender, Daniel Gruhl, 森本典繁, Anthony Lu/日経エレクトロニクス 1997.2.24な

どにも開示されている。そこで、まずパッチワーク法の原理を説明する。

【0052】

パッチワーク法では画像に対して統計的偏りを生じさせることによって付加情報 $E_s(H)$ の埋め込みを実現している。

【0053】

図5を用いて、パッチワーク法の原理を説明する。同図において、原画像から2つの部分集合AとBを選択する。今、部分集合Aは部分集合 $a_{i \in 01}$ に代表される複数の部分集合からなり、部分集合Bは部分集合 $b_{i \in 02}$ に代表される複数の部分集合からなるとする。

【0054】

この2つの部分集合は互いに重ならなければならない、本実施の形態におけるパッチワーク法による付加情報 Inf の埋め込みが実行可能である。

【0055】

今、部分集合A、Bはそれぞれ、 $A = \{a_1, a_2, \dots, a_N\}$ 、 $B = \{b_1, b_2, \dots, b_N\}$ で表されるN個の要素からなる集合であるとする。部分集合Aと部分集合Bの各要素 a_i 、 b_i は画素値を持つ画素または画素の集合を表しているとする。

【0056】

ここで、次の指標 d を次のように定義する。

$$d = 1/N \cdot \sum (a_i - b_i)$$

ここで、 \sum は $i = 1 \sim N$ に関する和である。

【0057】

これは、2つの集合の画素値の差の期待値を示している。

【0058】

一般的な自然画像に対して、適当な部分集合Aと部分集合Bを選択し、指標 d を定義すると、Nは十分大きな値の場合には、

$$d \approx 0$$

となる性質がある。以降では、この d を信頼度距離と呼ぶ。

【0059】

一方で、付加情報 $E_s(H)$ を構成する各ビットの埋め込み操作として、例えば“1”のビット情報を埋め込む場合、

$$a'_i = a_i + c$$

$$b'_i = b_i - c$$

という操作を行う。これは部分集合 A の全ての要素の画素値に対して「c」を加え、部分集合 B の全ての要素の画素値に対して「c」を減ずるという操作である。なお、本実施形態では、以降、この「c」の値を“埋め込み深さ”と呼ぶ。

【0060】

ここで、先程の場合と同様に、付加情報 $E_s(H)$ が埋め込まれた画像から部分集合 A と部分集合 B を選択し、指標 d を計算すると、次の通りになる（各 Σ は $i = 1 \sim N$ の総和である）。

$$\begin{aligned} d &= 1/N \cdot \Sigma (a_i - b_i) \\ &= 1/N \cdot \Sigma \{ (a_i + c) - (b_i - c) \} \\ &= 1/N \cdot \Sigma \{ (a_i - b_i) + 2c \} \\ &\doteq 2c \end{aligned}$$

つまり、0 から一定距離離れた値となる。

【0061】

他方のビット情報（“0”のビット情報）を埋め込む場合には、

$$a'_i = a_i - c$$

$$b'_i = b_i + c$$

の操作を行う。すると、信頼度距離 d は、

$$\begin{aligned} d &= 1/N \cdot \Sigma (a_i - b_i) \\ &= 1/N \cdot \Sigma \{ (a_i - c) - (b_i + c) \} \\ &= 1/N \cdot \Sigma \{ (a_i - b_i) - 2c \} \\ &\doteq -2c \end{aligned}$$

となり、0 から負の方向へ一定距離はなれた値となる。

【0062】

即ち、ある画像が与えられた場合に、画像に対して信頼度距離 d を算出することにより、付加情報が埋め込まれているかを判断することができる。

【 0 0 6 3 】

信頼度距離 $d \equiv 0$ ならば付加情報 $E_s(H)$ は埋め込まれておらず、信頼度距離 d が0から一定量以上離れた正の値であるなら、1のビット情報が埋め込まれており、 d が0から一定量以上離れた負の値であるなら、0のビット情報が埋め込まれていると判断できることを意味する。

【 0 0 6 4 】

本実施形態では、上記パッチワーク法の原理を応用し、1つの画像に複数のビットの情報を埋め込む。

【 0 0 6 5 】

本実施形態では、1つの画像の互いに異なる領域に、部分集合AとBの組み合わせだけでなく、部分集合A'とB'、部分集合A''とB''、…という複数の組み合わせを想定することで、複数のビットからなる付加情報 $E_s(H)$ を埋め込む。ただし、部分集合AとB、部分集合A'とB'、部分集合A''とB''、…の配置は、お互いに重なり合わないことが必要である。

【 0 0 6 6 】

ここで、複数のビット情報が埋め込まれたデータから、ビット情報を抽出する方法について考えてみる。

【 0 0 6 7 】

図6の601は、電子透かしが埋め込まれていないデータから計算される信頼度距離 d の分布を示している。分布0601は、信頼度距離 d の地点に対応する出現頻度分布が大きなほど、出現しやすい信頼度距離 d の値であることを示している。

【 0 0 6 8 】

分布602、分布603は、それぞれ1、0のビット情報を埋め込んだデータから計算される信頼度距離 d の分布を示している。同様に信頼度距離分布602、603でも同様に信頼度距離 d の地点に対応する出現頻度分布が大きいほど、出現しやすい信頼度距離 d の値であることを示している。なお、一つの信頼度距離 d は一つのビット情報に対応している。

【 0 0 6 9 】

ここで、図6の601、602、603は、全て正規分布になっている。その理由を中心極限定理を用いて説明する。

【0070】

<中心極限定理>

平均値 m_c 、標準偏差 σ_c の母集団（正規分布でなくても良い）から大きさ n_c の任意標本を抽出した時、標本平均値 S_c の分布は n_c が大きくなるにつれて正規分布 $N(m_c, (\sigma_c/\sqrt{n_c})^2)$ に近づくことを示す定理である。

【0071】

一般には母集団の標準偏差 σ_c は不明なことが多いが、サンプル数 n_c が十分大きく、母集団の数 N_c がサンプル数 n_c に比べてさらに十分大きいときは標本の標準偏差 S_c を σ_c の代わりに用いても実用上ほとんど差し支えない。

【0072】

本実施の形態において、部分集合A、Bは夫々 $A = \{a_1, a_2, \dots, a_N\}$ 、 $B = \{b_1, b_2, \dots, b_N\}$ で表されるN個の要素からなる集合で、夫々図5に示される様な部分集合Aと部分集合Bの要素の持つ画素値とする。信頼度距離 $d(\sum(a_i - b_i)/N)$ は、Nが十分大きな値を取り、画素値 a_i と b_i には相関がない場合は、信頼度距離 d の期待値は0になる。また中心極限定理から、信頼度距離 d の分布は正規分布をとることが分かる。

【0073】

従って、信頼度距離 d から埋め込まれたビット情報を判断する場合に、0と信頼度距離 $2c$ の間に適当な閾値を導入し、信頼度距離の絶対値が、閾値よりも大きい場合に埋め込みがあると判断することで、統計的に十分信頼できる情報の抽出が可能になる。

【0074】

例えば、正規分布601の標準偏差を σ とすると、付加情報の埋め込みがない場合には、図6の斜線部分で示す $-1.96\sigma \sim +1.96\sigma$ の区間（95%の信頼区間）に信頼度距離 d は95%の確率で出現する。

【0075】

従って、閾値の値を大きくすると、閾値の外に出現する信頼度距離 d の確率は

低くなり、信頼性の高い情報の抽出が可能になる。

【0076】

また、埋め込み深さ「c」を大きくすると、正規分布602、603はから遠ざかり、閾値を大きくすることも可能になる。

【0077】

また部分集合AとBの要素数Nを大きくすると、正規分布601、602、603の標準偏差 σ が小さくなるため、同じ埋め込み深さcでも、より信頼性が高くなる。

【0078】

以上がパッチワーク法の基本的な考え方である。

【0079】

本実施の形態では、電子透かし埋め込み部204、電子透かし抽出部302は、以上で説明したパッチワーク法を用いている。

【0080】

以下、電子透かしの埋め込み、抽出、除去の具体的な方法を説明する。

【0081】

＜埋め込み位置決定部＞

パッチワーク法では、複数ビットからなる付加情報を埋め込むため、1つのビット情報ごとに部分集合AとBが必要になる。従って、複数のビット情報を埋め込む場合には、AとB、A'とB'、A''とB''、…の位置を決定する必要がある。

【0082】

図4の埋め込み位置決定部401では、複数のビットを埋め込むのに必要な埋め込み位置を決定する。埋め込み位置の決定方法としては、簡単なものとしては乱数を用いて決める方法が考えられる。各部分集合の要素がほぼ等しくなるようにし、部分集合がお互いに重なりあわず、画像全体にバランスよく埋め込まれることが好ましい。

【0083】

一例として、画像と同じ大きさを有するホワイトノイズマスクを利用する方法

について簡単に述べる。

【 0 0 8 4 】

ホワイトノイズマスクは2次元的にマスク画素が配置され、それぞれのマスク画素は0～255の係数を持つ。ホワイトノイズマスクの0～255の各々の係数には、それぞれ略等しい数のマスク画素が割り当てられる。

【 0 0 8 5 】

例えば、原画像が2000×2000画素(=4000000画素)である場合、ホワイトノイズマスクのマスク画素も同じだけ用意することになるので、例えば0の値を持つマスク画素は、 $4000000 / 256 = 15625$ 個存在することになる。他の値を持つマスク画素も同じである。これらのマスク画素が乱数的に散りばめられたものをホワイトノイズマスクとするのである。

【 0 0 8 6 】

従って、1ビットの付加情報を埋め込む場合には、奇数の値を持つマスク画素を部分集合Aに割り当て、偶数の階調を持つマスク画素を部分集合Bに割り当てると、部分集合Aと部分集合Bの要素が等しく、重なり合わず、画像全体にバランスよく埋め込むことが可能になる。

【 0 0 8 7 】

M個からなる複数のビットの情報を埋め込む場合には、各ビットあたりに割り当てる画素の数を、1～Mのビット情報あたりに等しく割り当てる(例えば、ホワイトノイズマスクの取り得る範囲を2Mで割り、その剰余を部分集合AまたはBに用いるなどして均等に割り当てる)ことにより、複数のビット情報の埋め込みが可能になる。

【 0 0 8 8 】

画素が8ビットで表される場合、階調数は256となるので、埋め込み可能な最大ビット数Mは128となる。ハッシュ値(64ビットとか128ビット)のみの場合には、これで十分であるが、例えば、それ以外の情報(例えば著作権保護のための情報)を追加しようとするとき足りなくなる場合がある。しかし、原画像を4分割し、それぞれの分割ブロックについて、それぞれのホワイトノイズマスクを設定すれば、 $128 \times 4 = 512$ ビットを埋め込むことが可能となる。ま

た、4分割ではなく、それ以上にすれば埋め込みビット数を増やすことも可能である。ただし、分割数を多くすると、逆に、正規分布になりずらくなるので、埋め込み情報の抽出が失敗することもあり得る。従って、原画像のサイズに応じて分割数を決定するようにすればよい。

【 0 0 8 9 】

従って、埋め込み位置決定部は、例えば予め用意されたマスクパターンを発生するだけで良いことになる。なお、電子透かしの抽出分離する側では、埋め込みで用いたマスクと同じものを用意しておき、これを利用することになる。

【 0 0 9 0 】

＜付加情報埋め込み部＞

付加情報埋め込み部 4 0 2 には、先に説明したように、画像データ I および、付加情報 E s (H)、埋め込み位置決定部 4 0 1 で決定された各ビットに対応する埋め込み位置が入力される。

【 0 0 9 1 】

入力される付加情報 E s (H) を構成するビット情報に従って各ビットに対応する部分集合 A と B の画素の画素値を操作する。

【 0 0 9 2 】

上述のパッチワーク法の説明で述べたように、ビット情報が 1 の場合には、部分集合 A の画素の画素値に「c」を加え、部分集合 B の画素の画素値から「c」を減じる。ビット情報が 0 の場合には、部分集合 A の画素の画素値から「c」を減じ、部分集合 B の画素の画素値に「c」を加えることになる。付加情報埋め込み部 4 0 2 では、以上の操作により、付加情報 E s (H) の埋め込みを行う。

【 0 0 9 3 】

以上説明した方法で付加情報の埋め込みを行うことが可能であるが、前記方法を実行した場合、 $c > a_i$ または、 $a_i > 255 - c$ 、及び、 $c > b_i$ または、 $b_i > 255 - c$ となる画素においては、埋め込み後の画素値 a_i' 、及び b_i' が、 a_i' 、 $b_i' < 0$ 、或いは、 a_i' 、 $b_i' > 255$ となる。すると、後述する電子透かし除去部において、これらの画素については原画像の画素（即ち、 a_i 及び b_i ）を復元することが出来ない。

【 0 0 9 4 】

よって本実施の形態においては、 $c \leq a_i \leq 255 - c$ 、及び $c \leq b_i \leq 255 - c$ となる画素に埋め込み処理を実行し、この範囲外の画素値に対しては埋め込み処理を行わない。従って、先にMビットを埋め込む場合、先に「ホワイトノイズマスクの取り得る範囲を2Mで割り」と説明したが、この範囲を除外する必要がある。なお、これらの埋め込み処理を実行しない画素の位置情報をオーバーフロー位置情報として出力し、後述する電子透かし抽出部、及び電子透かし除去部に入力する必要がある。

【 0 0 9 5 】

＜電子透かし抽出手段＞

次に、本実施形態における電子透かし抽出部302について説明する。電子透かし抽出部302は、例えば、図7に示す構成になっている。

【 0 0 9 6 】

図示の様に、電子透かし抽出部302は、埋め込み位置決定部701、付加情報抽出部702、統計検定部703、比較部704、付加情報除去部705から構成される。

【 0 0 9 7 】

はじめに、電子透かし抽出部に、電子透かし埋め込みデータ wI' が入力される。次に埋め込み位置決定部701では、電子透かしが埋め込まれている位置情報（電子透かし埋め込み部204で使用したホワイトノイズマスクと同じパターン）を発生する。次の付加情報抽出部702では、入力される電子透かしが埋め込まれている位置情報を基に、電子透かし埋め込みデータに対し、所定の処理を施すことによって、画像データ wI' に埋め込まれている付加情報 $E's(H)$ に対応する信頼度距離 d を計算する。次の統計検定部703では、付加情報抽出部702で計算された付加情報 $E's(H)$ に対応するデータの確からしさを、統計的に検定する。充分正確な付加情報 $E's(H)$ であると判定された場合には、比較部704により付加情報 $E's(H)$ の抽出を行う。確からしくなければ情報なしと出力する。情報が埋め込まれている場合には、入力された画像データ wI' 、埋め込み位置決定部702からの埋め込み位置情報、及びオーバーフロ

一位置情報を用いて、付加情報除去部 7 0 5 において電子透かしが除去される。

【0 0 9 8】

次に、電子透かしが埋め込まれた画像データ wI' からこの付加情報 $E's(H)$ を抽出する電子透かし抽出部の動作について詳細に述べる。

【0 0 9 9】

＜埋め込み位置決定部＞

埋め込み位置決定部 7 0 1 において、画像データ wI' 中のどの領域から付加情報 $E's(H)$ を抽出するかを決定する。この埋め込み位置決定部 7 0 1 によってなされる動作は、前述した埋め込み位置決定部 4 0 1 と同じであり、その為、4 0 1 と 8 0 1 によって決定される埋め込み位置は同一のものとなる。決定された埋め込み位置の情報は、付加情報抽出部 7 0 2、及び付加情報除去部 7 0 5 に出力される。

【0 1 0 0】

＜付加情報抽出部＞

付加情報抽出部 7 0 2 では、埋め込み位置決定部 7 0 1 で決定された埋め込み位置から各ビットに対応する信頼度距離 d を計算する。この際に、入力されたオーバーフロー位置情報に従い、ここに示されている画素には付加情報は埋め込まれていないため、信頼度距離 d の算出には用いない。

【0 1 0 1】

＜統計検定部＞

統計検定部 7 0 3 では、付加情報抽出部 7 0 2 から出力されるそれぞれのビット情報に対応する信頼度距離 d に対して、確からしさを統計的に検定する。複数ビットの情報を埋め込んでいる場合には、複数の信頼度距離 d が得られる。付加情報 $E's(H)$ が埋め込まれている場合には、信頼度距離 d は図 6 では、中心 0 から離れた位置 $2c$ を中心とした位置に出現する。

【0 1 0 2】

このとき、埋め込み深さ c が大きければ大きいほど、信頼度距離 d は図 6 において、中心 0 から離れて出現する。従って、「 c 」の位置に閾値を導入し、「 c 」よりも大きな信頼度距離 d が得られる場合には、埋め込まれたビット情報は 1

であり、 $-c$ よりも小さな信頼度距離 d が得られる場合には埋め込まれたビット情報は0であると判断できる。

【0103】

従って、付加情報の埋め込み時に埋め込み深さ「 c 」が大きければ大きいほど、正規分布601、602および603の間隔が広がり、抽出情報の信頼性が高くなる。また部分集合AおよびBの要素数 N が大きければ大きいほど、正規分布601、602および603の標準偏差は小さくなる。従って、埋め込み深さ「 c 」および部分集合AおよびBの要素数 N を大きくすることで、閾値が「 c 」の場合でも抽出情報の信頼が高く設定できる。

【0104】

なお、埋め込みがない場合の信頼度距離 d は $-c \sim c$ の小さな区間に全て出現する（しやすい）ので、それを利用して判断する。

【0105】

すなわち、本実施形態の統計検定部703では、複数のビットに対応する信頼度距離 d がある一定以上、 $-c \sim c$ の範囲に出現する場合には、情報が埋め込まれていないと判断し、その旨を表示する。

【0106】

<比較部>

図7の比較部704には、付加情報抽出部702と統計検定部703を経て出力された各ビット情報に対応する信頼度距離 d の値が供給される。

【0107】

比較部704に入力される各ビット情報に対応する信頼度距離 d は信頼性の高い情報であるので、各ビット情報に対応する信頼度距離 d の正または負の符号から、“1”または“0”の何れであるかを単純に判定するだけで良い。

【0108】

具体的には、付加情報 $E's(H)$ を構成するあるビット情報の信頼度距離 d が「 c 」より大きい場合、このビット情報が“1”であると判定し、信頼度距離 d が「 $-c$ 」より小さい場合はこのビット情報が“0”であると判定する。

【0109】

<付加情報除去部>

付加情報除去部 7 0 5 で行なわれる操作を説明する。付加情報除去部 7 0 5 に
は、付加情報 $E's (H)$ の埋め込み位置、画像データ wI' 、及びオーバーフ
ロー位置情報が入力され、付加情報が除去された画像データ I' が出力される。

【0 1 1 0】

電子透かし埋め込み部における付加情報埋め込み部 4 0 2 で行った埋め込みを
行った位置と同一の位置で、各ビットに対応する部分集合に対し、埋め込み深さ
 c を埋め込み時とは符号を反対にして加えることで、付加情報を除去し、原画像
を復元する。

【0 1 1 1】

具体的には、付加情報 $E's (H)$ を構成する所定のビット情報の埋め込み位
置において、ビット情報が 1 である場合、

$$a'_i = a_i - c$$

$$b'_i = b_i + c$$

の処理を行い、ビット情報が 0 の場合には、

$$a'_i = a_i + c$$

$$b'_i = b_i - c$$

の処理を行うことで、それぞれ埋め込み前の画素値に復元することが可能になる
。この際に、入力されたオーバーフロー位置情報に従う。従ってオーバーフロー
位置である画素には付加情報は埋め込まれていないため、除去の対象にはしない
。

【0 1 1 2】

以上で述べた操作を行い、付加情報除去部 7 0 5 は、電子透かし埋め込みデー
タ wI' から電子透かしを除去し、電子透かしが除去された画像データ I' を出力
する。

【0 1 1 3】

以上の実施形態においては、認証情報としてデジタル署名を用いる方法につ
いて説明したが、本発明はこれに限定されることなく、例えば認証情報として M
A C (メッセージ認証符号) を用いる方法も含まれることも明らかである。更に

、デジタル署名、或いは、MACに加えて、日付情報、位置情報、時間情報、装置の固有情報、署名者の固有情報のうち少なくとも一つ以上を含むことも可能である。

【0114】

更に、以上の実施の形態において、付加情報には誤り訂正符号化されたものを用いることも可能であり、そうする事によって、更に抽出された付加情報Infの信頼性を向上させることができる。

【0115】

なお、上述した情報を埋め込む側、及び、埋め込まれた情報を認証する側の装置は、そのほとんどがソフトウェアでもって実現できる。すなわち、図2、図3に示す各処理部はソフトウェアで構成できる。

【0116】

この場合、装置構成は、一般のパーソナルコンピュータ等の汎用装置で良く、その一例を示せば図1の構成とすることができる。

【0117】

同図は本実施の形態に適用する画像処理装置の全体構成を示したものである。本図において、ホストコンピュータ101は例えば一般に普及しているパーソナルコンピュータである。

【0118】

ホストコンピュータ101の内部では、バス107により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。

【0119】

図中、103は、内部の各ブロックの動作を制御、或いは内部に記憶されたプログラムを実行することのできるCPUである。104は、ブートプログラムやBIOSを記憶しているROMである。105はCPUにて処理を行うために一時的にプログラムや処理対象の画像データを格納しておくRAMである。106は、RAM等に転送されるプログラム(OSや画像処理プログラム)や画像データをあらかじめ格納したり、処理後の画像データを保存することのできるハードディスク(HD)である。署名装置として機能する場合には、このハードディス

ク106には、図2に対応するプログラムが格納され、RAM105にロードされ実行されることになる。また、認証装置として機能する場合には、図3に示す構成に対応するプログラムがこのハードディスク106に格納され、RAM105にロードされ実行されることになる。

【0120】

108は、外部記憶媒体の一つであるCD（CD-R）に記憶されたデータを読み込み或いは書き出すことのできるCDドライブである。109は、108と同様にFDからの読み込み、FDへの書き出しができるFDドライブである。110も、108と同様にDVDからの読み込み、DVDへの書き出しができるDVDドライブである。尚、CD、FD、DVD等に画像編集用のプログラム、或いはプリンタドライバが記憶されている場合には、これらプログラムをHD106上にインストールし、必要に応じてRAM105に転送されるようになっている。これらの記憶媒体は、オリジナル画像を記憶させ、それに著名情報を埋め込むことに使用されたり、逆に、配布された記憶媒体内の著名付き画像について認証処理を行うことになる。

【0121】

113は、キーボード111或いはマウス112からの入力指示を受け付けるためにこれらと接続されるインターフェイス（I/F）である。また、114はグラフィックコントローラ及びビデオメモリ（不図示）を内蔵し、表示に関する制御を行う表示制御部であり、ビデオメモリに展開されたイメージデータを表示装置115に出力することで像を表示させる。115は通信インタフェースであり、インターネットに接続するためのものである（例えば、モデムやイーサネットボード等）。著名情報を付加した情報をこの通信インタフェース115で送信したり、或いは受信することも可能となる。

【0122】

なお、イメージデータを入力する手段として、上記に限らず、イメージスキャナ等でも構わないのは勿論である。

【0123】

以上のように、本発明は、複数の機器（例えばホストコンピュータ、インタフ

ェース機器、リーダー、プリンタ等) から構成されるシステムの 1 部として適用しても、1 つの機器 (例えば携帯端末や P D A 等) からなるものの 1 部に適用してもよい。

【 0 1 2 4 】

また、本発明は上記の如く、システム又は装置内のコンピュータ (CPUあるいは M P U) に、上記実施の形態を実現する為のソフトウェアのプログラムコードを供給し、このプログラムコードに従って上記システムあるいは装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【 0 1 2 5 】

またこの場合、前記ソフトウェアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給する為の手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【 0 1 2 6 】

この様なプログラムコードを格納する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、C D - R O M、磁気テープ、不揮発性のメモリカード、R O M等を用いることができる。

【 0 1 2 7 】

また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働している O S (オペレーティングシステム)、あるいは他のアプリケーションソフト等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【 0 1 2 8 】

更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに

備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【 0 1 2 9 】

以上説明した様に本実施形態によれば、デジタル情報と署名情報を不可分の状態とすることが可能であり、フォーマット変換などを介しても署名情報を認証装置に送信することが可能となる。

【 0 1 3 0 】

【発明の効果】

以上説明したように本発明によれば、認証情報をデジタル情報と不可分にしつつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのデジタル情報に復元することが可能になる。

【図面の簡単な説明】

【図 1】

実施形態で適用可能なコンピュータのブロック構成図である。

【図 2】

実施形態における署名装置のブロック構成図である。

【図 3】

実施形態における認証装置のブロック構成図である。

【図 4】

図 2 における電子透かし埋め込み部の詳細を示す図である。

【図 5】

パッチワーク法の原理を説明するための図である。

【図 6】

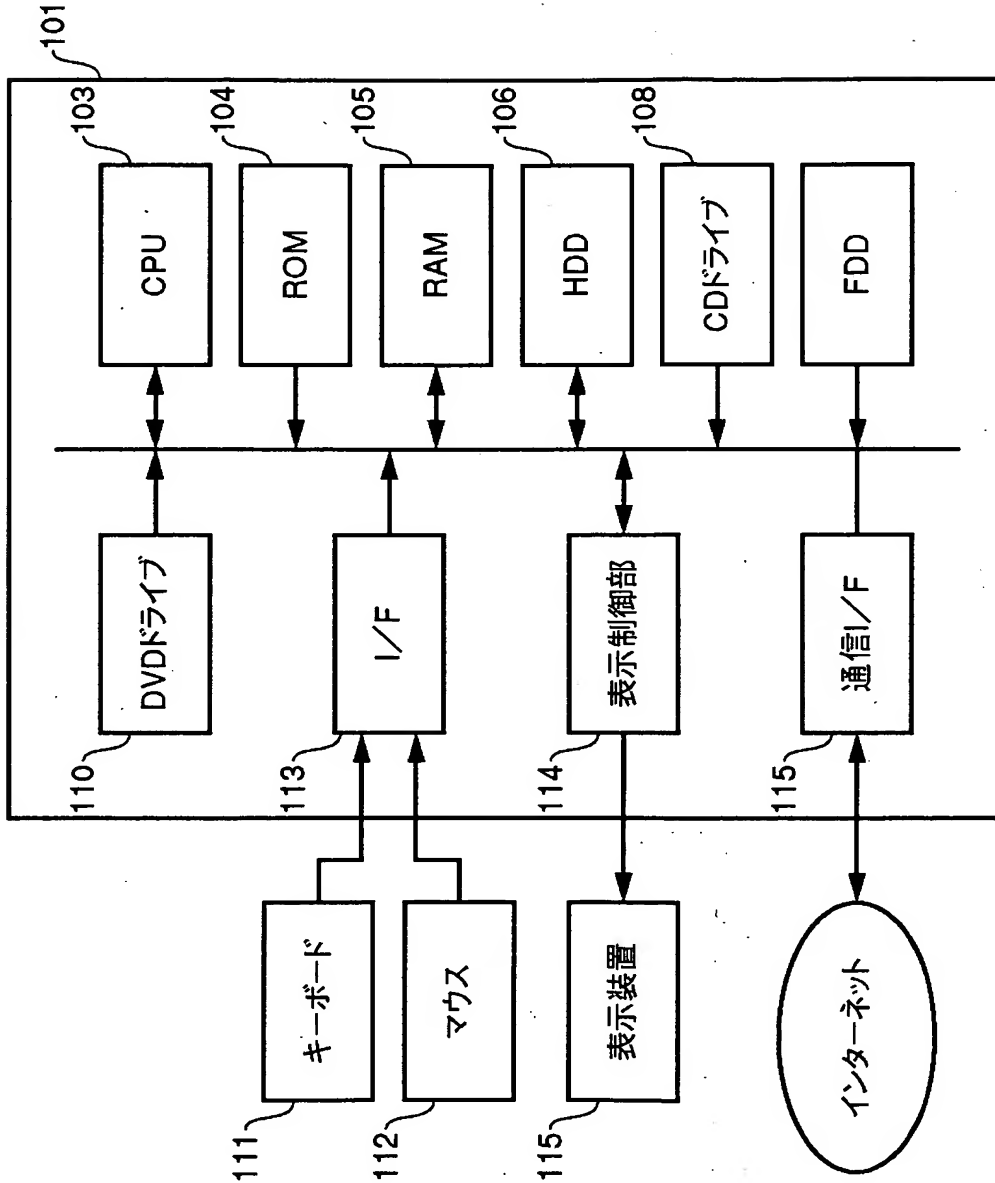
電子透かし抽出時の信頼度距離 d の出現頻度分布を示す図である。

【図 7】

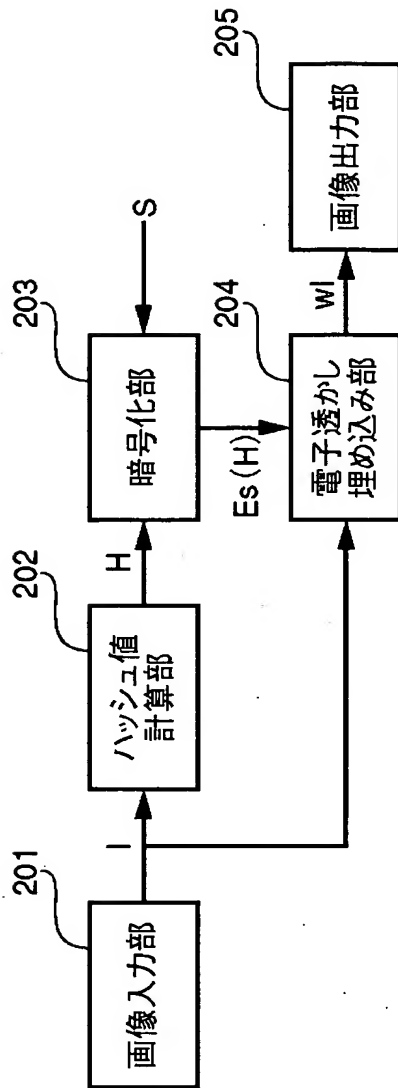
実施形態における電子透かし抽出部のブロック構成図である。

【書類名】 図面

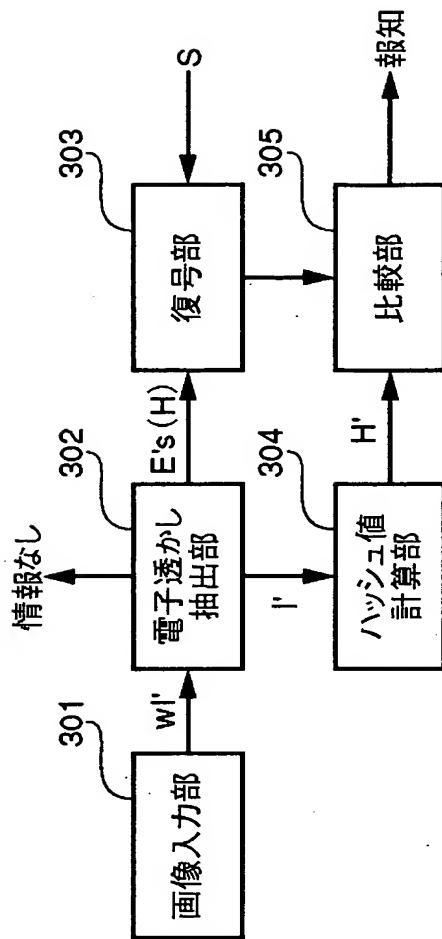
【図 1】



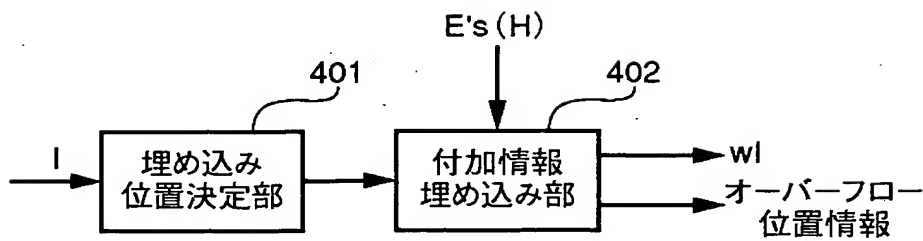
【図 2】



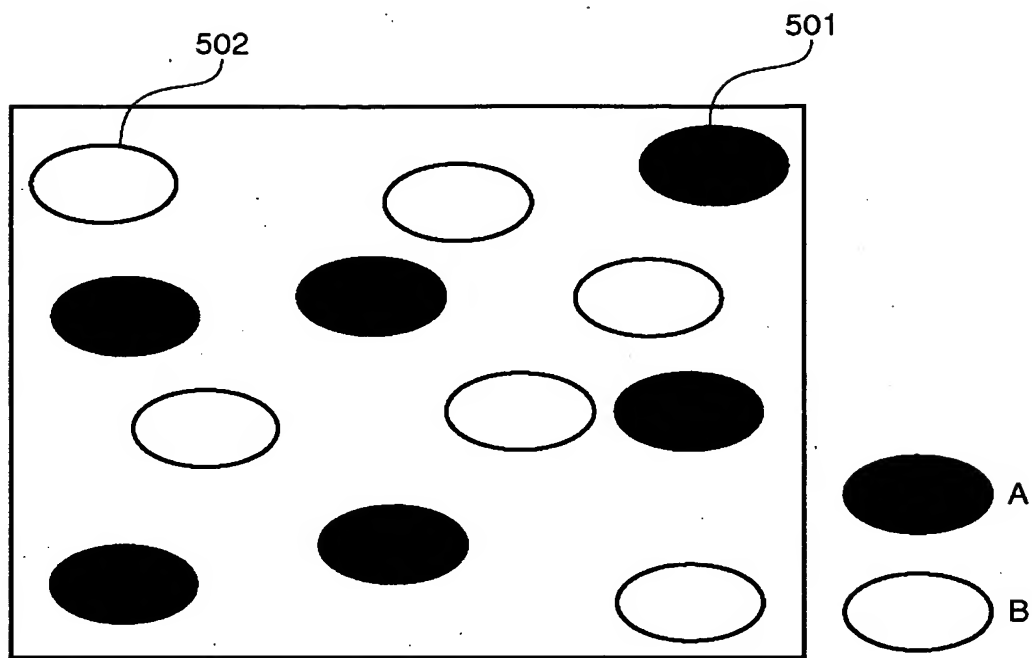
【図 3】



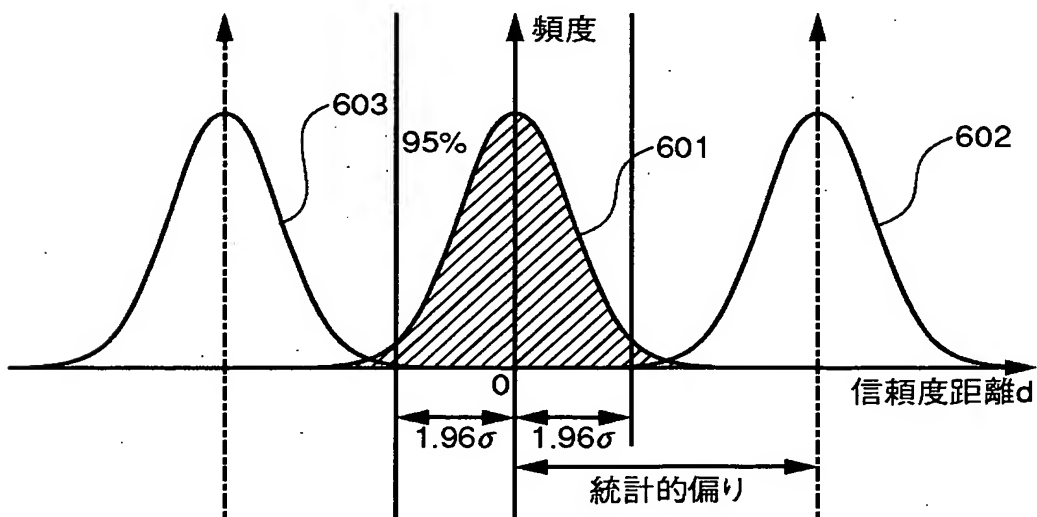
【図 4】



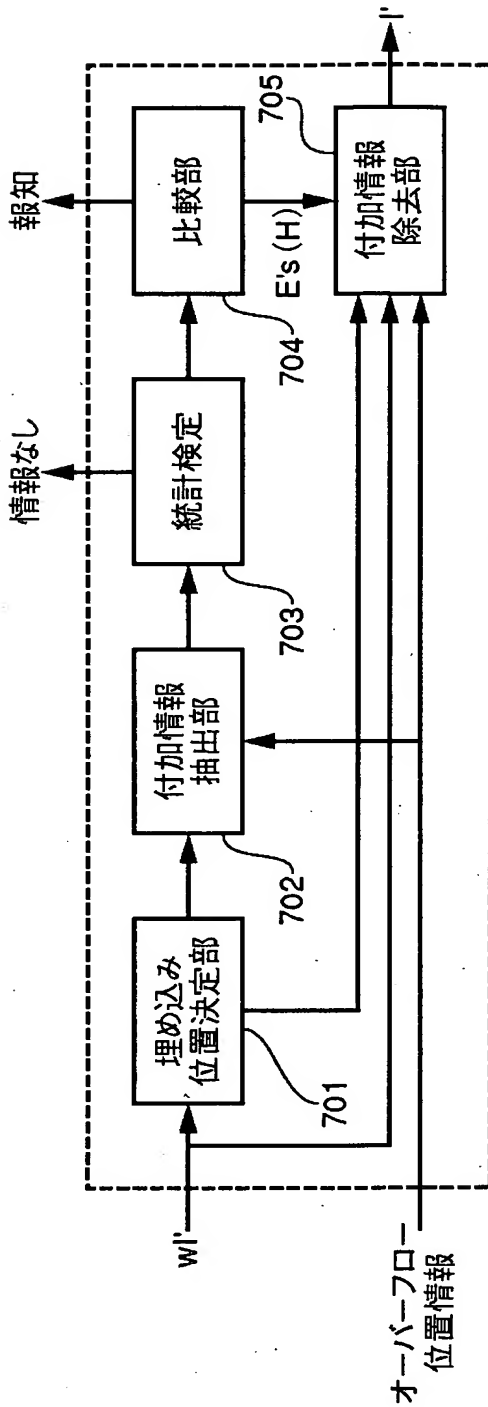
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 認証情報をデジタル情報と不可分にししつ、改ざんがなされているか否かを判断でき、しかも改ざんがない限りはオリジナルのデジタル情報に復元することを可能にする。

【解決手段】 画像入力部201より入力したデジタル情報に認証情報を埋め込む場合、そのデジタル情報に基づいてハッシュ値計算部202で認証情報を生成し、暗号化部203で暗号化鍵で暗号化し、電子透かし埋め込み部204で、それをデジタル情報に電子透かしとして埋め込む。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都大田区下丸子3丁目30番2号
氏 名 キヤノン株式会社